



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1430
Alexandria, Virginia 22313-1430
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/461,984	12/15/1999	JIN LU	PHA-23-890	4517

24737 7590 04/06/2006

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER

HOFFMAN, BRANDON S

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 04/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/461,984	Applicant(s) LU ET AL.	
	Examiner Brandon S. Hoffman	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 17 January 2006.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-29 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-29 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-29 are pending in this office action.
2. In view of the appeal brief filed on January 17, 2006, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

- (1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,
- (2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

4. Claims 1-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kim et al. (U.S. Patent No. 5,799,081) in view of Zhang et al. (U.S. Patent No. 6,550,008), and further in view of Applicant's Admitted Prior Art (AAPA).

Regarding claims 1, 2, 8, 13, and 18, Kim et al. teaches a system/method/
deployment module/host device/article of manufacture for copy protecting information,
the system comprising:

- A point of deployment module (fig. 4, ref. num 22); and
- A set-top box including (fig. 4, ref. num 20);
- Wherein the set-top box transmits a request message for information (fig. 21, host device transfers EMM, ECM, and CPTC to smart card), and
- The point of deployment module generates a reply message (fig. 21, smart card responds by sending CW).

Kim et al. does not teach the control information pair includes CCI and a stream identifier, generating a first key in the POD module and a second key in the set-top box, the point of deployment module encrypting the information with the first shared key and transmitting the encrypted information to the set-top box, and the set-top box decrypting the encrypted information with the second shared key when the first and second shared keys match.

Zhang et al. teaches the point of deployment module encrypting the information with the first shared key and transmitting the encrypted information to the set-top box (col. 10, lines 22-25), and the set-top box decrypting the encrypted information with the second shared key (col. 10, lines 25-29).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the POD encrypting the information with the first shared key and transmitting the information to the set-top box, and the set-top box decrypting the information, as taught by Zhang et al., with the system of Kim et al. It would have been obvious for such modifications because shared session keys, used for symmetric key cryptosystems, provide authentication of devices as well as keeping data secure.

The combination of Kim et al. as modified by Zhang et al. does not teach the reply message including at least one control information pair, each pair having copy control information and a stream identifier; generating a first shared key in the deployment module and a second shared key in the set-top box; and decrypting the content when the shared key match.

AAPA teaches the reply message including at least one control information pair, each pair having copy control information and a stream identifier (page 2, paragraph 2 through 4 of specification, the definition of an elementary stream is that it contains a stream ID in the header of each elementary stream, coupled with the CCI used for each elementary stream, as suggested by AAPA); generating shared keys in the deployment module and the set-top box (page 2, end of second paragraph of specification); and decrypting the content when the shared key match (page 3, first paragraph of specification).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a control information pair, generating shared keys, and decrypting content when the shared key match, as taught by AAPA, with the system of Kim et al./Zhang et al. It would have been obvious for such modifications because shared session keys, used for symmetric key cryptosystems, provide authentication of devices as well as keeping data secure.

Regarding claims 3, 9, and 14, the combination of Kim et al. as modified by Zhang et al./AAPA teaches wherein the deployment module is selected from the group consisting of a point of deployment module, wireless data interface appliance, smartcard, personal computer, or Internet interface appliance (see col. 3, line 16 of Zhang et al.).

Regarding claims 4, 10, and 15, the combination of Kim et al. as modified by Zhang et al./AAPA teaches wherein the host is a set-top box (see col. 1, line 28 of Zhang et al.).

Regarding claim 5, the combination of Kim et al. as modified by Zhang et al./AAPA teaches wherein the encryption means includes a hash function (see col. 10, lines 36-39 of Zhang et al.).

Regarding claim 6, the combination of Kim et al. as modified by Zhang et al./AAPA teaches wherein the encrypted information in an elementary stream of information is encrypted with the first shared key (see fig. 4, step num 9 of Zhang et al.).

Regarding claims 7, 25, and 28, the combination of Kim et al. as modified by Zhang et al./AAPA teaches wherein the stream identifier that is transmitted to the host is incorporated with the Packetized Elementary Stream (PES) header of the elementary stream (see page 2, paragraph 2-4 of specification of AAPA).

Regarding claims 11 and 16, the combination of Kim et al. as modified by Zhang et al./AAPA teaches wherein the encrypted information is transmitted to the host device using a transport stream, wherein the transport stream includes at least one elementary stream (see page 2, paragraph 2 through 4 of specification of AAPA).

Regarding claims 12 and 17, the combination of Kim et al. as modified by Zhang et al./AAPA teaches wherein respective ones of the at least one control information pairs is associated with respective ones of the at least one elementary streams (see page 2, paragraph 2-4 of specification of AAPA).

Regarding claim 19, the combination of Kim et al. as modified by Zhang et al./AAPA teaches wherein to use the at least one control information pair in the generating of said second key the set-top box receives a transmission of said at least

one control information pair, the respective copy control information of said at least one control information pair not being encrypted for the transmission (see col. 19, lines 63-67 of Kim et al., it would stand to reason that the control information is unencrypted so that it can be utilized by the host quickly).

Regarding claim 20, the combination of Kim et al. as modified by Zhang et al./AAPA teaches wherein step b) is executed without encrypting said copy control information of said at least one control information pair (see col. 19, lines 63-67 of Kim et al.).

Regarding claim 21, the combination of Kim et al. as modified by Zhang et al./AAPA teaches wherein said copy control information of said at least one control information pair in the reply message is unencrypted upon transmission to the host device (see 19, lines 63-67 of Kim et al.).

Regarding claim 22, the combination of Kim et al. as modified by Zhang et al./AAPA teaches wherein the information to be encrypted comprises content information (see col. 10, lines 22-25 of Zhang et al.).

Regarding claim 23, the combination of Kim et al. as modified by Zhang et al./AAPA teaches wherein said content information comprises content information of an

elementary stream, said stream identifier being an identifier of an elementary stream (see fig. 4, step num 9 of Zhang et al.).

Regarding claims 24 and 27, the combination of Kim et al. as modified by Zhang et al./AAPA teaches wherein said stream identifier uniquely identifies an elementary stream that is assigned said copy control information (the CW and CP of Kim et al. (fig. 21) will identify the copy control information uniquely assigned with the stream identifier).

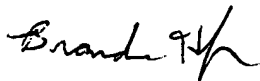
Regarding claims 26 and 29, the combination of Kim et al. as modified by Zhang et al./AAPA teaches wherein the encrypted information to be transmitted to the set-top box includes said header, said set-top box being configured to retrieve said stream identifier from said header (see fig. 21, ref. num 263 of Kim et al., uses CW to decrypt the information.).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

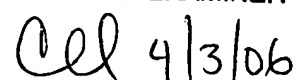
Art Unit: 2136

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



BH

CHRISTOPHER REVAK
PRIMARY EXAMINER



4/3/06